REMARKS

This amendment is responsive to the Office Action dated January 4, 2005. Applicants have cancelled claims 3, 10 and 11, and amended claims 1, 2, 4-9, 12, 14-16, 19 and 20. Claims 1, 2, 4-9 and 12-20 are pending.

Amendments to the Specification

Applicants have amended the specification to address the informalities raised by the Examiner.

Claim Objections

In the Office Action, the Examiner objected to claim 15. Applicants have amended claim 15 to address the informalities raised by the Examiner.

Claim Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over Jardin (USPN 6,681,327) in view of Narad (USPN 6,157,955). Applicants respectfully traverses the rejection to the extent such rejections may be considered applicable to the claims as amended. The applied references fail to disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Claims 1 and 7

Applicants have amended claim 1 to require discarding at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record. Applicants have amended claim 7 to require buffering a portion of the decrypted application data and discarding a remaining portion prior to authenticating the application data. Neither Jardin nor Narad teach or suggest these or other elements of claims 1 and 7.

With respect to claims 1 and 7, the Examiner correctly acknowledges that Jardin fails to teach or suggest authenticating decrypted packet application data of a security record on receipt of a final packet of the security record. Nevertheless, the Examiner states that it would have been

obvious to a person of ordinary skill in the art at the time of the invention to modify the Jardin system in view of the teachings of Narad to authenticate packet application data on receipt of a final packet of a segment.

In contrast, Narad describes a general-purpose packet processing system that includes a Policy Engine (PE) that applies policy decisions to packets based on the results of a packet Classification Engine (CE). Narad makes no mention of authenticating a security record or application data that spans multiple packets when receiving the final packet at all. The "cryptographic key" referenced by the Examiner is described by Narad in reference to cryptographic unit that generally supports encryption and decryption. The "checksum" described by Narad is merely used to determine whether a packet is valid or corrupted in some form. Narad makes no mention of authenticating a security record or authenticating application data that spans multiple packets at all.

Consequently, neither Jardin nor Narad, either separately or in combination, teach or suggest a method in which an intermediary apparatus forwards decrypted, unauthenticated application data to a server, discards at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record, and authenticates the decrypted packet application data of the security record on receipt of a final packet of the security record, as required by amended claim 1.

Similarly, neither Jardin nor Narad, either separately or in combination, teach or suggest forwarding decrypted application data, buffering a portion of the decrypted application data and discarding a remaining portion prior to authenticating the application data, and authenticating the remaining application data when the information for authenticating the application data is received in the last of the multiple packets, as required by Applicant's amended claim 7.

Moreover, Applicants submit that even if the Jardin system were modified to include a form of authentication, the modified system would still not achieve Applicants' claim. In particular, Jardin recognizes that conventional SSL techniques are commonly used for the authentication. For example,

> SSL provides the mechanism to implement authentication and encryption. Authentication ensures that each of the client and server is who it claims to be. In practice, authentication may simply involve entering a user identification (ID) and password. However, a computer hacker may eavesdrop on the client-server link to intercept password and user name information. Encryption deters such mischief by

> scrambling the user ID and password information before transmission over the network. In addition to encrypting user information, SSL uses encryption to secure nearly every type of data including the payload (i.e., a text document) communicated between the client and server. In effect, SSL provides for encryption of a session, and authentication of a server, message, and optionally a client.[1]

Further, Jardin states:

> When a client and server wish to communicate using a SSL connection, they exchange information about a protocol version, select cryptographic algorithms, authenticate each other, and use public-key encryption techniques to generate shared secrets. These processes are handled by the handshake protocol of the SSL connection... .[2]

Conventional SSL authentication techniques utilize a message authentication code (MAC) algorithm in which TCP/IP packets are buffered until a complete SSL record is formed.[3] Once a complete SSL record is formed, the application data carried by the SSL record is decrypted and authenticated. Once authenticated, the application data may then be processed by the application layer and communicated to a destination server, e.g., via TCP/IP packets.

Consequently, even in view of Narad or conventional SSL authentication, it would not have been obvious to one of ordinary skill in the art to modify the Jardin system to forward decrypted, unauthenticated application data for a security record to the server, discard at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record, and authenticate the security record on receipt of a final packet of the security record, as is required by claim 1.

Similarly, it would not have been obvious to one of ordinary skill in the art to modify the Jardin system in view of Narad to forward the decrypted application data as the multiple packets are decrypted, buffer a portion of the decrypted application data while discarding the remaining portion prior to authenticating the application data, and authenticate the remaining portion of the application data when the information for authenticating the application data is received in the last of the multiple packets, as required by claim 16.

---

[1] Col. 1, ll. 49-63 (emphasis added).
[2] Col. 4, ll. 47-53 (emphasis added).
[3] See, e.g., the Background of the present application.

Claim 4 and 12

With respect to claims 4 and 12, neither Jardin nor Narad teach or suggest buffering the remaining portion of the packet application data as a minimal length sufficient to complete a block cipher used to encrypt the data.

The Examiner's is correct that Jardin describes dynamically allocating the buffer size in response to traffic volume between clients and servers; however, allocation in response to traffic volume is unrelated to allocation for a minimal length sufficient to complete a block cipher used to encrypt the data as required by Applicants' claims. The Examiner has failed to identify any portion of Jardin that discusses any correlation between the buffer size and the block cipher size. Moreover, given that the buffer is used in the Jardin system to store incoming application data until a data transport connection can be established, Jardin suggests that the buffer is extremely large, unrelated to the block cipher size and, therefore, not a minimal length sufficient to complete a block cipher used to encrypt the data, as required by Applicants' claims 4 and 12.

Claims 5 and 19

With respect to claims 5 and 19, the Examiner correctly acknowledges that Jardin fails to teach or suggest authenticating decrypted packet application data of a security record on receipt of a final TCP segment. For at least the reasons set forth above, Narad fails to teach or suggest authenticating the decrypted data for the security record upon receiving a final TCP segment of a multi-segment encrypted data stream and after forwarding the decrypted, unauthenticated application data received prior to the final TCP segment, as required by claim 5. Similarly, Narad fails to teach or suggest authenticating the data on receipt of a final segment of the SSL encrypted data after forwarding the unauthenticated application data that is received prior to the final segment, as required by claim 19.

Claims 6 and 14

With respect to claim 6, as explained above, the Examiner is correct that conventional SSL utilizes a failure alert in the event an authentication failure is encountered for an SSL record. However, as described above, conventional SSL authentication utilizes a message MAC algorithm in which TCP/IP packets are buffered until a complete SSL record is formed.[4] Once a complete SSL record is formed, the application data carried by the SSL record is block decrypted

[4] See, e.g., the Background of the present application.

and authenticated. Once authenticated, the block of application data may then be communicated to a destination server, e.g., via TCP/IP packets.

Neither Jardin, Narad or conventional SSL techniques suggest notifying the client apparatus if a failure in authenticating the security record occurs after already forwarding and discarding at least a portion of the decrypted, unauthenticated application data to the server, as required by Applicants' claim 6. Similarly, neither Jardin, Narad or conventional SSL techniques suggest alerting a first device if authenticating fails after forwarding and discarding at least a portion of the decrypted, unauthenticated application data that is received prior to the last one of the multiple packets, as required by claim 14.

Claims 16

With respect to claim 16, Jardin fails to teach or suggest buffering encrypted data in a memory buffer in a device, the buffer having a length equivalent to a block cipher size necessary to perform the cipher. In rejecting claim 16, the Examiner again cited Jardin at col. 6, ll. 9-14. As clarified above, this passage of Jardin clearly states that the broker of the Jardin system buffers incoming application data "until a handshake can be used to establish a data transport connection between the broker 120 and the server 130a."

The Examiner has failed to identify any portion of Jardin that discusses an actual buffer size let alone any correlation between the buffer size and the block cipher size. Moreover, given that the buffer Jardin is to store incoming application data until a data transport connection can be established, Jardin clearly suggests that the buffer is extremely large, unrelated to the block cipher size and, therefore, not "equivalent to the block cipher size necessary to perform the cipher," as required by Applicants' claim 16. Thus, in contrast to the Examiner's assertion, Jardin fails to teach or suggest a method for providing secure communications using limited buffer memory in which a buffer having a length equivalent to a block cipher size necessary to perform the cipher, as required by Applicants' claim 16.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicants' claims 1-20 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

Application Number 09/900,493
Responsive to Office Action mailed January 4, 2005.

Rejection for Double Patenting:

The Examiner provisionally rejected claims 1-5, 7-13 and 15-19 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-30 of copending Application No. 09/900,496. In addition, the Examiner provisionally rejected claims 1-5, 7-13 and 15-19 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-30 of copending Application No. 09/900,496 in view of Narad.

Applicants note the provisional status of this rejection. Accordingly, Applicants will address this issue if and when the rejection is formally applied.

CONCLUSION

All claims in this application are in condition for allowance. Applicants respectfully request reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: April 4, 2005

By:

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312